Purdue University
Center for Education and Research in Information Assurance and Security

Top Research Challenges in InfoSec

<http://www.cerias.purdue.edu>

Eugene H. Spafford
Director

Topics

- Context of current networked environment
- What are the concerns?
- Top technological challenges
- A few closing observations

Computers & communications

- Capacity doubles per year, but some delays stay nearly constant (speed of light).
- Speed
  - in 1974 was 1000 bits per second
  - in 1984 was Megabits per second
  - in 1994 is Gigabits per second
  - in a few years is expected to be Terabits/sec
- Human bit rate is now exceeded. This is leading to an information revolution.

Basic Infrastructure

- Experimental protocols
- Interconnection of smaller networks
- Commodity software/hardware

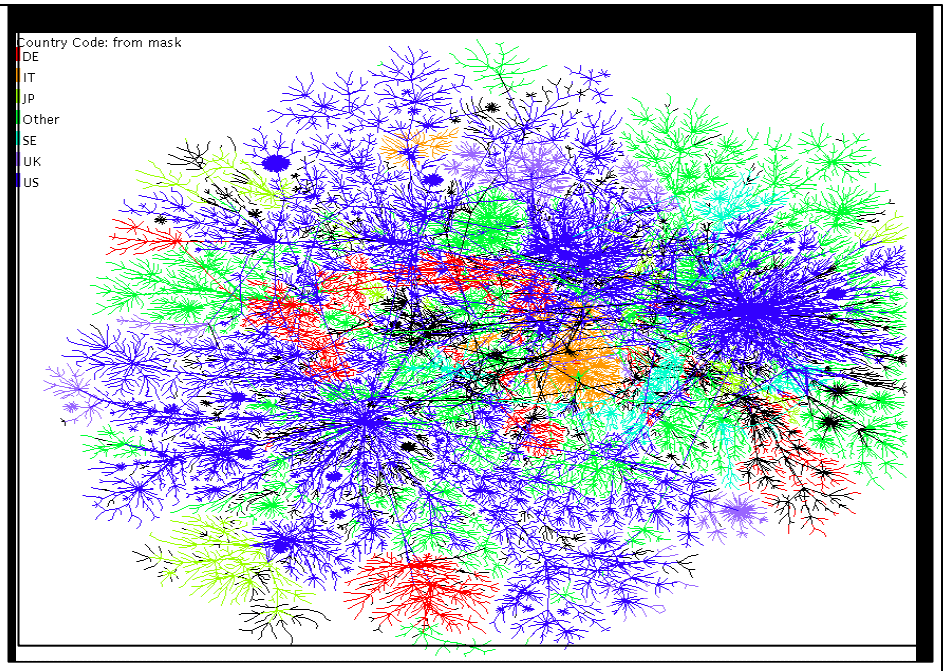
Seven years ago there was no commercial use of the net.

10 years ago, there were less than 75,000 machines connected.

The workstation is about 15 years old.

The Information 4-Lane Today

- Millions of systems on all continents; As of June 2, 2000, there were 17,737,054 registered domains.
- In excess of 250 million users have access
- Over 150 countries around the world have registered for access
- Population doubling in less than 10 months for last 11 years
- Volume of traffic doubling every 90 days



www.cybergeography.org

Population change

- Doubling every 6-10 months. Thus:
  - Over half have less than 1 year of experience.
  - Less than 5% of users have 5+ years experience.
  - Fewer than 1% have 10+ years experience.
- Was technologists, mostly literate, college educated, dedicated
- Now includes a broader mix including those of questionable education & intent, tyros & tyrants

Topics

- Context of current networked environment
- What are the concerns?
- Top technological challenges
- A few closing observations

Coming soon

The pace of change is increasing. Consider technology already being marketed or tested:

- Smaller, portable systems
- Wireless computing
- Multimedia on demand
- Constant connections
- “Free” communications
- Radical new architectures
- Private data warehousing

Future Environment

- World-wide
- High speed networking
- Cheap (free?), ubiquitous computing
- Widely-deployed encryption
- Truly mobile computing

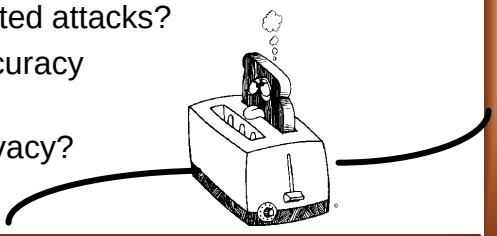
The Information Highway in 2004

- At current rate of growth, every human on Earth will have access.
- Some studies project 250 computers in the home, car and office for every adult in North America.
  - This includes home appliances and utilities in “smart houses.” This may lead to “ToasterNet”
  - May include semi-automatic highways, with navigation, collision avoidance, etc.
- Universal addresses/phone numbers
- Radio, TV, 3-D, Virtual Reality Broadcasts

These will all be networked together!

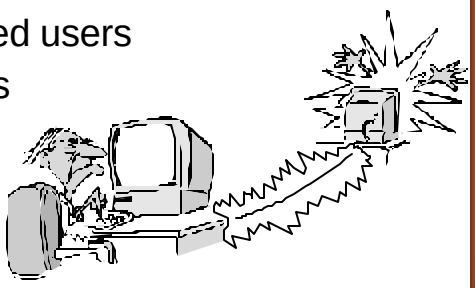
Problems with ToasterNet

- How can I protect my household systems against 250 million network users?
- How can businesses protect against fraud, theft, extortion, vandalism?
- How do we protect against organized and distributed attacks?
- How do we control accuracy and quality?
- How do we protect privacy?



Computer Criminals

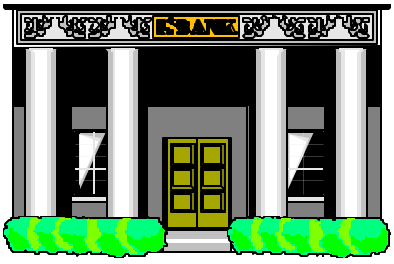
- Hackers “joyriding”
- Industrial espionage
- National espionage
- Canonical disgruntled users
- Terrorists/Anarchists
- Organized Crime



On why he robbed banks:

“That’s where the money was.”

- *Willie Sutton, famed bank robber*



Topics

- Context of current networked environment
- What are the concerns?
- Top technological challenges
- A few closing observations

Non-crime, non-technical issues

- Privacy concerns
- Encryption issues
- Trans-national law enforcement issues
- Taxation issues
- Intellectual property issues
- “Sunshine” laws
- Mandatory access laws

Nature of Challenges

- Rapidly-changing environment
- Large installed base of legacy systems
- Few research professionals
- No “one size” solutions likely
- Government interference & regulation will complicate the solution space
- Increasing non-national threats
- Looming issues of trans-national interests

So, what are the big technological challenges?

1. Composable Policy

- Simple expression of policies
- Policy traceable to features
- Intranets to Extranets and back again
- Reliable auditing and natural language expression
- Policy “libraries”

2. Reliable Metrics

- How secure is my system?
- How secure is my network?
- Is a change worthwhile?
- What is the affect of adding new exposure?
- How can I balance protection level with cost?

3. Affordable High Assurance

- Secure “out of the box”
- Retrofit to legacy applications
- Available to small firms as well as large
- Both hardware and software assurance
- Repeatable, measurable assurance and quality

4. Assured Availability

- Resistance to attack
- Resistance to failure
- Automatic reconfiguration & recovery
- Graceful degradation under attack
- Formal models of availability and Quality of Service (QoS)

5. Accurate Risk Data

- How likely is a threat?
- How likely is an attack?
- How likely is a failure?
- Provide feedback to policy decisions
- How to collect, classify, and organize appropriately?

6. Graceful Penetration Tolerance

- Attacked but contained
- Automatic reconfiguration
- Fallback configurations and systems
- Automatic deployment of recovery mechanisms

7. Automated Response

- Respond to attacks
- Don’t respond in error
- Respond only enough to contain or stop
- Integrate with other systems’ responses
- Also satisfy law-enforcement needs
- Automated “strike-back” is not an option

8. Forensics

- Who is coming across the network?
- Where are they coming from?
- Legally-supportable evidence
- What did that software do?
- Who wrote that virus?
- What happened?
- How did it happen?
- Automated analysis of attacks

9. Identification and Authorization

- Portable on-line ID
- Authorization without Identification
  - Short-term
  - Permanent
- PKI and Public Keys
  - Availability
  - Interrelationship
  - Dynamic keys
  - Revocation management

10. Useful Audit Trails

- What needs to be logged from
  - Host
  - Applications
  - Network
- How do we store it?
- Dynamic auditing and reconstruction

11. Models

- For over 12 years, focus has been on the “Orange Book” and its progeny (MLS).
- This model doesn’t work for networks, object-based systems, thin clients, and active content.
- What model should we use?
- What alternatives can we create?
- How will that model adapt to future architectures?

12. Multimedia Security

Systems are processing different kinds of data than text and numbers.

How do we secure systems involving:

- Real time video
- Audio
- Multi-media databases
- Active content
- Remote processing

Topics

- Context of current networked environment
- What are the concerns?
- Top technological challenges
- A few closing observations

Outlook: Challenging

- We are faced with myriad problems in a rapidly-changing environment, with insufficient resources and a severe shortage of qualified personnel.
- The market is not ready for or supportive of necessary fundamental change
- Users don't generally accept basic principles
- Supply of quality professionals is limited

The real challenges?

Biggest challenges may be political and social rather than technical

- Global, not national network
- What is appropriate use?
- Whose laws govern?
- What is the standard language/culture?
- Taxation?
- Who pays for infrastructure for the poorer users?

Do we understand trust?

- A web page existing should not instill trust
- Taking electronic payments should not instill trust
- Being run by a government should not instill trust
- Software should not be trusted simply because it comes from a major developer
- How do you develop trust in someone you've never met anywhere but "Cyberspace"?

The importance of privacy

- Abuses of privacy will turn people away. Privacy protection must be designed in as a first principle.
- Protect my data
- Protect the data about me
- Protect the information about what I access
- Treat me as an individual

…Privacy can be a selling point

The role of quality

More will continue to be lost to bugs, disasters, and misuse than any crime.

- Because computers are simple to use does not mean they are safe
- When will quality become a selling point instead of a liability?
- When will lawyers & insurance companies take the initiative away from us?

An overlooked infrastructure

- We do not and will not have enough experts
- Not a simple business case
- Government not interested (yet)
- Disparity with industry is severe
- Recognition as a discipline is lagging
- Hiring “hackers” is not a good choice in most cases
- Disasters may be required to prompt action


CERIAS
Center for Education and Research in Information Assurance and Security
Thank you!
Email: <spaf@cerias.purdue.edu>
WWW: <http://www.cerias.purdue.edu>